IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF 3970 Mount Olivet Road. Martinsville, Virginia 24112	Case No. ___4:21mj17_____

Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jason P. McCoy, a Special Agent with the Federal Bureau of Investigation being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Richmond, Virginia, Field Office, Lynchburg Resident Agency. I have been employed with the FBI since July 2019 and as a law enforcement officer since 2007. Prior to joining the FBI, I was a Special Agent with the United States Air Force Office of Special Investigations and began conducting federal criminal investigations after completing the Federal Law Enforcement Training Center's (FLETC) Criminal Investigator Training Program (CITP) in September 2012. As part of my duties, I investigate criminal violations relating to child exploitation, in violation of 18 U.S.C. § 2251 and violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A. I have experience in the area of child pornography and child sexual exploitation investigations and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media. I also have experience in interviewing and

interrogation techniques, arrest procedures, search warrant applications, the execution of searches, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this affidavit, which includes the entire residence and property located at 3970 Mount Olivet Road, Martinsville, Virginia 24112, and any containers and storage buildings found on the curtilage of the property, any vehicles belonging to Clayton RIDDLE, and any electronic devices found on the person of Clayton RIDDLE whether at the SUBJECT PREMISIS or with law enforcement during the execution of the search, (the "SUBJECT PREMISES AND PERSON"), as well as the contents of electronic devices located on the SUBJECT PREMISES AND PERSON, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, which are more specifically described in **Attachment B** of this affidavit.

3. The statements contained in this affidavit are based in part on information provided by U.S. federal law enforcement agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative and federal grand jury subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not

included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located at the SUBJECT PREMISES AND PERSON.

DEFINITIONS

4. The following definitions apply to this affidavit:

a. "Kik" is a freeware instant messaging mobile app from the Canadian company Kik Interactive, and available free of charge on iOS and Android operating systems. It is a social networking application that permits a user to trade and disseminate various forms of digital media while using a cellphone. Kik advertised itself as "the first smartphone messenger with a built-in browser." Kik was founded in 2009 and according to its company website was designed to "break down barriers [between operating systems] that would allow users to chat with whoever, whenever." In October 2019, Kik Interactive was purchased by Santa Monica, California based MediaLab Inc. MediaLab Inc. is a holding company that owns other internet-based communication applications such as Whisper, Datpiff and others.

b. "Kik Messenger" is a feature within Kik that allows its users to communicate with selected persons as well as browse and share any website content with those whom the user selects while still within the Kik platform. Unlike other messaging apps, Kik usernames - not

phone numbers - are the basis for Kik user accounts. Kik usernames are unique; can never be replicated; can never be changed, may include lower and uppercase letters, numbers and/or periods and underscores; will never contain spaces, emoticons or special characters. A Kik username is the only publicly available identifier MediaLab Inc. can use to identify a Kik account to law enforcement. The company cannot identify users using phone numbers, first and last name (display name), or email address.

c. "Group": In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users (with whom the user selects) or publicly (on the Kik platform) with multiple individuals who belong to Groups. Groups are formed when like-minded individuals join collectively online in an online forum, created oftentimes by a Kik user designated as the Kik "Administrator" of the group. Groups can hold up to 50 Kik usernames. Groups are created to host/discuss topics such as modern popular culture-themed ideas as well as illicit/illegal-themed ideas. Public groups names are a user-generated hashtag; can never be replicated; can never be changed; may include lower and uppercase letters, numbers and/or periods and underscores; will never contain spaces, emoticons or special characters; The group hashtag will begin with a hash (#) (i.e. #AffidavitForWarrant).

d. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as internet forums and email.

e. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

f. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involves the use of a minor engaged in sexually explicit conduct, (b) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and specifically includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1)

h. The "Domain Name System" or "DNS" is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

i. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

j. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

m. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of

eighteen years.

o. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

q. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

r. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

s. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text

Transport Protocol (HTTP).

BACKGROUND ON CHILD PORNOGRAPHY AND COMPUTERS

5. I have had both training and experience in the investigation of computer-related crimes and child pornography crimes. Based on my training, experience, and knowledge, and the knowledge of more experienced agents, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. Smartphones and other mobile computing devices use mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive,

store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

6. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via the Internet:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g. online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES AND PESON as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

7. Based on all of the information contained herein, I believe that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via the Internet. In particular, the target of investigation, Clayton RIDDLE, used the Kik Messenger Application, joined a group named #c.hild.p.orn and distributed online child sexual abuse and exploitation material to the group administrator.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

8. A user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly sent and received child pornography via Kik Messenger. There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES used the Kik Messenger Application, joined a group named #c.hild.p.orn, and distributed online child sexual abuse and exploitation material (CSAM) to the group administrator. There is probable cause to believe that this Internet user is Clayton RIDDLE.

9. On August 19, 2020, FBI Online Covert Employee (OCE) was operating on Kik as an adult male when he joined Kik group #c.hild.p.orn. On October 11, 2020, a Kik user with the username cj10000000p00000 (Courtney) sent a video of toddler being sexually abused by two males. Specifically, the video showed a prepubescent female being orally penetrated by an adult male, while another adult male anally penetrated her. This visual depiction of sexually explicit conduct involving a minor meets the definition of child pornography under Title 18 of the United States Code. FBI Agents monitoring the Kik Group #c.hild.p.orn watched activity within the group of members who were posting and trading Child Sexual Abuse Material (CSAM) and electronically witnessed cj10000000p00000 (Courtney) send this video of CSAM to the Kik Group Administrator. Specifically, when cj10000000p00000 (Courtney) entered the Group, the Administrator sent a message to cj10000000p00000 (Courtney) which stated “verify”. Courtney responded “how”. The Administrator responded, “usual way”. cj10000000p00000 (Courtney) responded by uploading the previously described video. The Administrator responded, “good to go”.

10. On October 20, 2020, MediaLab responded to a subpoena for records related to the following Kik user: cj10000000p00000. The following was noted: Email-claytonriddle93@gmail.com; Username-cj10000000p00000; Recent IP (Internet Protocol Address defined in paragraph 4)-"69.244.224.22" – Comcast; "76.1.172.111"- CenturyLink, Comcast.

11. On October 26, 2020, Centurylink responded to a subpoena related to "ip":"76.1.172.111", "remotePort":"56045" which indicated the subscriber is: LONNIE O RODGERS JR (deceased), 970 Mount Olivet Road, Martinsville, Virginia 24112, Telephone number 276-634-5313, email address rodgerscarolyn@yahoo.com.

12. A review of public records revealed the land parcel corresponding with 970 Mount Olivet Road, Martinsville, Virginia is owned by the Chatmoss Country Club. Specifically, the 970 parcel is part of the golf course.

13. Public record revealed the address corresponding with Lonnie O. Rodgers and Carolyn Rodgers is 3970 Mount Olivet Road, Martinsville, Virginia 24112. The residence located at this address is owned by Carolyn Rodgers. Virginia DMV records show the current residents of 3970 Mount Olivet Road are Carolyn Rodgers and Clayton James RIDDLE. Public records indicate that Rodgers is RIDDLE's grandmother.

14. On May 21, 2021, Google responded to a subpoena related to the email address claytonriddle93@gmail.com. Google disclosed the email address is registered to Clayton RIDDLE, unincorporated, Virginia 24112. Google pay records indicate a Mastercard ending in 2420 on file as of July 4, 2018, belonging to Clayton RIDDLE. The previous card on file was a Visa card ending in 8579 also belonging to Clayton RIDDLE. This card was deleted on April,

17, 2018. Carolyn Rodgers' Mastercard ending in 5744 was also on file and was deleted from the account on May 11, 2018.

15. On October 29, 2020, Comcast responded to a subpoena related to "ip":"69.244.224.22", "remotePort":"55891" which indicated the subscriber is: HEATHER HOFFMAN, 4084 Mount Olivet Road, Martinsville, VA 24112.

16. A review of public records revealed the residence located at 4084 Mount Olivet Road, is owned by Clifford and Heather Hoffman. Virginia DMV records indicate that in addition to Clifford and Heather Hoffman, William Hardy Pierce also resides at 4048 Mount Olivet Road. 4084 Mount Olivet Road is situated three houses down from the SUBJECT PREMISES.

17. On July 12, 2021, FBI spoke with members of the Henry County Sheriff's Office who disclosed that a Sergeant employed by the Henry County Jail since 2014 was a neighbor of RIDDLE's and had direct knowledge of RIDDLE and RIDDLE's whereabouts. The Sergeant stated he knows RIDDLE to reside at 3970 Mount Olivet Road and frequently sees RIDDLE in and around the residence. Furthermore, the Sergeant has witnessed RIDDLE exit the residence and walk to the Hoffman residence, located at 4048 Mount Olivet Road, where RIDDLE enters through the basement and appears to remain inside for long periods of time.

18. The facts as outline above provide investigators with the reasonable belief that Clayton James RIDDLE, who resides at 3970 Mount Olivet Road, and controls the email account claytonriddle93@gmail.com, joined a group named #c.hild.p.orn on October 11, 2020, and distributed online child sexual abuse and exploitation material (CSAM) to the Group Administrator. Furthermore, based on my training and experience pertaining to individuals who

access the internet with the intent of viewing child pornography, the reasonable belief exist that evidence of child pornography or child sexual abuse and exploitation material (CSAM) will be found at 3970 Mount Olivet Road, Martinsville, Virginia 24112.

19. In addition, Kik is a messenger application and not a storage medium. Images sent and received via Kik will be stored directly on the Computer, phone, or device with which the Kik user is communicating via Kik Messenger.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

20. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES AND PERSON, in whatever form they are found. One form in which the records are likely to be found is data stored on a Computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of Computers as well as a search of the data stored on those Computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

21. I submit that if a Computer or electronic storage media are found on the SUBJECT PREMISES AND PERSON, there is probable cause to believe that child pornography materials will be stored on that Computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a Computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a Computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, Computer storage media—in particular, Computers' internal hard drives—contain electronic evidence of how a Computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. As further described in Attachment B, this application seeks permission to locate not only Computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Computers and any storage medium in the SUBJECT PREMISES AND PERSON because: data on the storage medium can provide evidence of a file

that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices, or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

23. Information stored within a Computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a Computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the Computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the Computer was remotely accessed, thus inculpating or exculpating the Computer owner.

24. Further, Computer and storage media activity can indicate how and when the Computer or storage media was accessed or used. For example, Computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the Computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of Computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a Computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the Computer user. Last, information stored within a Computer may provide relevant insight into the Computer user's state of mind as it relates to the offense under investigation. For example, information within the Computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement). A person with appropriate familiarity with how a Computer works can, after examining this forensic evidence in its proper context,

draw conclusions about how computers were used, the purpose of their use, who used them, and when.

25. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, Computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the Computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

26. Further, in finding evidence of how a Computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent. I know that when an individual uses a Computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The Computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The Computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a Computer used to commit a crime of this type may contain data that is evidence of how the Computer was used; data that was sent or received; notes as to how the criminal conduct

was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

27. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that Computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search Computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching Computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of Computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with Computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched.

b. Searching Computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since Computer data is particularly vulnerable to inadvertent or intentional

modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many Computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within Computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, Computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

28. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of Computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless

routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

29. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying Computers (to include cellular phones as noted above) and storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

30. We also seek the court's permission to compel Clayton RIDDLE if present at SUBJECT PREMISES at the time of the execution of the search warrant to unlock any Computers

requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many Computers and electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a Computer or device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The Computer or device can then be unlocked if the front-facing camera detects a face with characteristics that match those of

the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a Computer or device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of Computers, especially users of cell phones, often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a Computer or device is engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

31. As discussed in this affidavit, your Affiant has reason to believe that one or more Computers will be found during the search. The passcode or password that would unlock the Computer(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the

Computers, making the use of biometric features necessary to the execution of the search authorized by this warrant.

32. I also know from my training and experience, as well as from information found in publicly available materials including those published by cellphone manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a Computer or device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple cellphones cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

33. Due to the foregoing, if law enforcement personnel encounter any Computers that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of RIDDLE to the fingerprint scanner of the computer; (2) hold the computer in front of the face of RIDDLE and activate the facial recognition feature; and/or (3) hold the computer in front of the face of RIDDLE activate the iris recognition feature, for the purpose of attempting to unlock the computer in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel RIDDLE to state

or otherwise provide the password or any other means that may be used to unlock or access the computers. Moreover, the proposed warrant does not authorize law enforcement to compel RIDDLE to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the computers.

CONCLUSION

34. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

35. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

/s/Jason P. McCoy
JASON P. McCOY
Special Agent

Federal Bureau of Investigation

Entered: July 20, 2021

Robert S. Ballou

Robert S. Ballou
United States Magistrate Judge